Discrete Mathematics 59 (1986) 191–198
North-Holland

COMMUNICATION

ENUMERATION WITH THE LATTICE OF PERIODS

Mauro CERASOLI
Dipartimento di Matematica, Università 67100 L'Aquila, Italy.

Communicated by G.-C. Rota
Received 5 November 1985

1. Introduction

Whenever a group G acts on the set $X = \{1, 2, \ldots, n\}$ a lattice $\mathcal{P}_n(G)$ of certain special partitions of X, called periods, associated with this action, can be defined. G.-C. Rota first presented this lattice in [6] and successively, with Smith in [9], used it to prove a generalization of Polya's enumeration theorem. The proof requires only the most elementary facts about permutation groups, plus the concept of Möbius inversion on a partially ordered set [5]. There are signs that the lattice of periods may be a useful tool in the enumerative combinatorics (i.e., enumeration under group action). In this paper we show another approach to this argument and some applications. In fact a combinatorial meaning of Jordan totient function will be given. For a probabilistic method to solve occupancy problems (or enumeration of functions between finite sets) without group actions, see [4].

2. The functions η and θ

Let be given the set $X = \{1, 2, \ldots, n\}$ and a group G of permutations of X, i.e., G is a subgroup of the symmetric group S_n. Let $L_n(G)$ be the lattice of all subgroups of G ordered by inclusion and let Π_n be the lattice of all partitions of X ordered by refinement. If $\alpha \in G$ is a product of cycles $C_1, C_2, \ldots, C_r$, we can write

$$\alpha = (C_1)(C_2)\cdots(C_r).$$

Moreover if $\pi \in \Pi_n$ has the blocks $B_1, B_2, \ldots, B_h$, we write

$$\pi = |B_1|\, B_2\, |\cdots|B_h|.$$

With 0 and 1 we denote respectively the minimum $|1\,|\,2|\cdots|n|$ and the maximum $|12\cdots n|$ of Π_n. If H is a subset of G, then $\langle H\rangle$ is the subgroup generated by H.

Now, let us define a function $\eta: G \to \Pi_n$. For every $\alpha \in G$ let be

$$\alpha = (C_1)(C_2)\cdots(C_r) \to \eta(\alpha) = |C_1 \mid C_2| \cdots |C_r|.$$

It is possible to extend the function η to subsets of G in the well known sense. If $H \subseteq G$, then

$$\eta(H) = \bigvee_{\alpha \in H} \eta(\alpha), \tag{2.1}$$

where the symbol $\vee$ means the sup-operation in the lattice Π_n.

If H is a subgroup of G, then we call $\eta(H)$ the period of H. In this case $\eta(H)$ is the partition of X equal to the set of orbits of H. If $\langle \alpha \rangle$ is the cyclic subgroup generated by α, then $\eta(\langle \alpha \rangle) = \eta(\alpha)$; moreover $\eta(G) = 1$ and $\eta(\langle \varepsilon \rangle) = 0$, when ε is the identity of G.

If we write the relation "a and b belong to the same block of partition π" by $a \equiv b \pmod{\pi}$, we can say that for every $a, b \in X$ and $H \subseteq G$,

$$a \equiv b \pmod{\eta(H)} \text{ iff at least } \alpha \in H \text{ exists such that } \alpha(a) = b.$$

The set of periods, or partitions of X, induced by subgroups of G, is denoted by $\mathscr{P}_n(G)$, i.e.,

$$\mathscr{P}_n(G) = \{\eta(H): H \in L_n(G)\}.$$

For the function η some properties hold which are reported in the following two propositions. The proofs, however, have been omitted.

Proposition 1. *Let $\eta: L_n(G) \to \Pi_n$ be the function defined by* (2.1), *then the following formulae hold, for every A, B, $A_i \in G$:*

(1) $A \subseteq B \Rightarrow \eta(A) \leqslant \eta(B)$,

(2) $\eta\left(\bigcup_{i=1}^{k} A_i\right) = \bigvee_{i=1}^{k} \eta(A_i)$,

(3) $\eta(A) \vee \eta(A^c) = 1$.

Proposition 2. *Given a function $f: G \to \Pi_n$, let be*

$$E(f) = \bigvee_{\omega \in G} [f(\omega) \wedge \eta(\omega)]$$

then

(a) $E(f \vee g) = E(f) \vee E(g)$, $E(f \wedge g) = E(f) \wedge E(g)$,

(b) *for every $\pi \in \Pi_n$ we have $E(\pi \wedge f) = \pi \wedge E(f)$.*

Together with the function η we can consider another function $\theta: \Pi_n \to L_n(G)$ defined as follows. For every $\pi \in \Pi_n$ we put

$$\theta(\pi) = \{\alpha \in G: \eta(\alpha) \leqslant \pi\}.$$

For example, $\theta(0)=\{\varepsilon\}$, $\theta(1)=G$. It is clear that $\theta(\pi)$ is a subgroup of G. Furthermore, we can say that $\theta(\pi)$ is the set of permutations of G that leave the blocks of π invariated, i.e.:

$$\theta(\pi)=\{\alpha\in G: a\equiv\alpha(a)\ (\mathrm{mod}\ \pi)\ \text{for every}\ a\in X\}.$$

In other words, the cycles of α are contained in the blocks of π.

Proposition 3. *For every* $\pi=|B_1\,|\,B_2|\cdots|B_h|\in\Pi_n$ *we have*

$$\theta(\pi)=G\cap[S(B_1^c)\cup S(B_2^c)\cup\cdots\cup S(B_h^c)],$$

where

$$S(B_i^c)=\{\alpha\in S_n:\ \alpha\in B_i^c\Rightarrow\alpha(a)=a\}.$$

3. Galois connection and periods

First of all, we have to recall an important result linking the functions η and θ (see [9]).

Proposition 4. *The functions* η *and* θ *satisfy the following properties*

(1) $H\subseteq\theta\eta(H)$ *for every* $H\in L_n(G)$,

(2) $\pi\leqslant\eta\theta(\pi)$ *for every* $\pi\in\Pi_n$.

Proof. The relation (1) is true because if $\alpha\in H$, then for $a\equiv b\ (\mathrm{mod}\ \eta(H))$ it results $b=\alpha(a)$ or $a=\alpha(b)$. This means that α leaves the blocks of $\eta(H)$ fixed, i.e., $\alpha\in\theta\eta(H)$. To show property (2) it must be considered that $a\equiv b\ (\mathrm{mod}\ \eta\theta(H))$ it is equivalent to say that there exists a $\beta\in\theta(\pi)$ such that $\beta(a)=b$. But if $\beta\in\theta(\pi)$, then $\beta(a)\equiv\alpha\ (\mathrm{mod}\ \pi)$, and the proof is completed. □

Now we can consider the lattice Π_n^* dual of Π_n, or with the inverse order. The functions η and θ in this case constitute a Galois connection (η,θ) between the lattices $L_n(G)$ and Π_n^*, as can be easily verified. A well-known fact about the functions $\theta\eta$ and $\eta\theta$ is the closure property, i.e., they are closure operators respectively on $L_n(G)$ and Π_n^* (see [2, p. 124]). It is useful to remember the definition of a closure operator on a set I. It is an application—defined on the subsets of I—such that for every A, $B\subseteq I$ it results:

(a) $A\subseteq\bar{A}$;

(b) $\bar{\bar{A}}=\bar{A}$;

(c) $\bar{A}\subseteq\bar{B}$ if $A\subseteq B$.

Now it follows that the closed partitions of X, respect to the operator $\eta\theta$, coincide with the periods defined above. In fact, if π is a closed partition, then

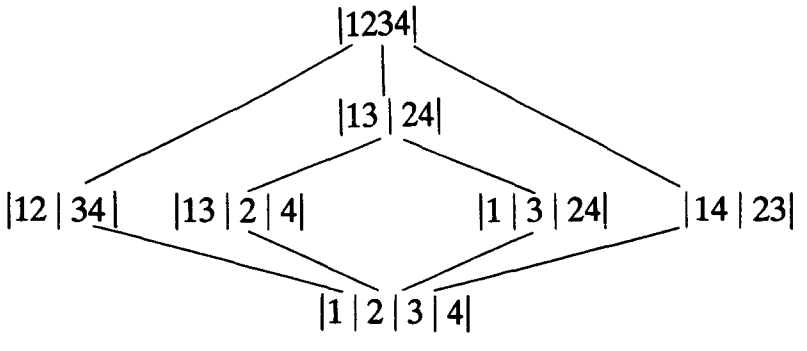
$\eta\theta(\pi) = \pi$ and therefore there exists a subgroup of G, say $H = \theta(\pi)$, such that $\eta(H) = \pi$. But then π is a period. It must be added that $\mathscr{P}_n(G)$, the set of periods, is really a lattice, since, it is well known that the closed elements of a closure space $(I, -)$ constitute a complete lattice. We will call the closed subgroups of G respect to the operator $\theta\eta$ periodics. Thus, the set of periodics subgroups is a complete lattice.

To give some examples of the concepts expounded above here follows an array in the case $n = 4$, $G = D_4$, the dihedral group on four elements, with $|\Pi_4| = 15$, see Table 1.

Table 1

π	$\theta(\pi)$	$\pi = \eta\theta(\pi)$
$\|1234\|$	D_4	π
$\|1 \mid 234\|$	ε, (24)	$\|1 \mid 24 \mid 3\|$
$\|134 \mid 2\|$	ε, (13)	$\|13 \mid 2 \mid 4\|$
$\|14 \mid 23\|$	ε, (14)(23)	π
$\|13 \mid 24\|$	ε, (13), (24), (13)(24)	π
$\|12 \mid 34\|$	ε, (12)(34)	π
$\|124 \mid 3\|$	ε, (24)	$\|1 \mid 24 \mid 3\|$
$\|123 \mid 4\|$	ε, (13)	$\|13 \mid 2 \mid 4\|$
$\|1 \mid 3 \mid 24\|$	ε, (24)	π
$\|13 \mid 2 \mid 4\|$	ε, (13)	π
others	ε	$\|1 \mid 2 \mid 3 \mid 4\|$

The Hasse diagram of $\mathscr{P}_4(D_4)$ is



Nevertheless, the classical example is given by $G = C_n$, the cyclic group on n elements, that is the group generated by the cycle $(12 \cdots n)$. In this case the lattice $\mathscr{P}_n(G)$ is isomorphic to the lattice of subgroups of C_n, or the lattice of divisors of n. The lattices of periods and periodics are not sublattices of Π_n and $L_n(G)$ respectively. For example, with $n = 6$ we have $|\Pi_6| = 203$, a Bell number, while with $G = C_6$ it results $|\mathscr{P}_6(C_6)| = 4$, because the subgroups of C_6 are only 4. We can note that the number of periods of X is small respect to the number of all partitions of X. Therefore the periods are very useful and important from a combinatorial point of view. In fact, for enumeration problems like Polya-Redfield type, it is convenient to work with the lattice $\mathscr{P}_n(G)$ instead of Π_n.

4. Aperiodics functions

Let Y be a finite set and $f: X \to Y$. The function f is said aperiodic respect to G, the permutation group on X, if $\alpha \in G$, $\alpha f = f$ implies $\alpha = \varepsilon$, the identity of G. In other words f is invariant only for the identity of G. Often, the elements of Y are called colors, so a function $f: X \to Y$ is a coloring of X. If the elements of X are vertices of a regular polygon and those of Y are pearls, then a function f is called a necklace.

If G is the cyclic group generated by $(12 \cdots n)$, that is the cyclic group of plane rotations of the polygon, respect to the centre, then a necklace is aperiodic if, by turning it, it is impossible to have an identical necklace, if the rotation is different from the identity ε.

To every $f: X \to Y$ we can associate the subgroup H_f of G, which is defined as follows:

$$H_f = \{\alpha \in G: \alpha f = f\}.$$

Therefore, H_f includes all permutations that leave f fixed. Then f is aperiodic if, and only if, $H_f = \{\varepsilon\}$. The period of H_f is called G-period of f; we denote it with $\mathrm{per}(f)$. In particular, if G is the symmetric group, the G-period of f coincides exactly with the kernel of f, i.e., the partition $\ker(f)$ such that $a \equiv b \pmod{\ker(f)}$ if, and only if, $f(a) = f(b)$. We note that if $\pi = \mathrm{per}(f)$, then f is constant on the blocks B_i of π, that is $|f(B_i)| = 1$ for every i.

Let A be an integral domain and $w: Y \to A$ a function, called weight. For all $f: X \to Y$ and $C \subseteq Y^X$ we set

$$w(f) = \prod_{k=1}^{n} w(f(k)); \qquad g(C) = \sum_{f \in C} w(f).$$

In this context, $g(C)$ is the enumerator, or generating polynomial, of C. We need of some properties satisfied by g. Let S and T be disjoints sets. Given $B = Y^S$, $C = Y^T$ let D be the product of B and C, i.e., the set of pairs $(f, h): S \cup T \to Y$, $f \in B$, $h \in C$, such that

$$(f, h)(a) = \begin{cases} f(a), & \text{if } a \in S \\ h(a), & \text{if } a \in T. \end{cases}$$

Then the relation $g(D) = g(B)g(C)$ obviously holds. We remember in the end a result useful for some future considerations.

Proposition 5 ([3, p. 112]). *Let* $\pi = |X_1 \,|\, X_2| \cdots |X_k|$ *be a partition of* X *and*

$$C = \{f \in Y^X: |f(X_i)| = 1 \text{ for every } i = 1, 2, \ldots, k\}.$$

Then

$$g(C) = \prod_{i=1}^{k} \sum_{y \in Y} w(y)^{|X_i|}.$$

5. Some combinatorial problems

Now, given a period π in $\mathcal{P}_n(G)$, let $A_w(\pi)$ be the generating polynomial of the functions $f: X \to Y$ with period π, i.e.,

$$A_w(\pi) = g(\{f \in Y^X : \mathrm{per}(f) = \pi\}).$$

The problem of determining a formula for $A_w(\pi)$ is solved in the following

Proposition 6. *If $\mu_{\mathcal{P}}$ is the Möbius function of the lattice $\mathcal{P}_n(G)$ and $X_i(\sigma)$, $i = 1, 2, \ldots, |\sigma|$, are the blocks of the partition $\sigma \in \Pi_n$, then*

$$A_w(\pi) = \sum_{\sigma \geqslant \pi} \mu_{\mathcal{P}}(\pi, \sigma) \prod_{i=1}^{|\sigma|} \sum_{y \in Y} w(y)^{|X_i(\sigma)|}. \tag{4.1}$$

Proof. We put $B_w(\pi) = g(\{f \in Y^X : \mathrm{per}(f) \geqslant \pi\})$ so that

$$B_w(\pi) = \sum_{\sigma \geqslant \pi} A_w(\sigma)$$

is the generating polynomial of the set of functions f having period π. Then any one of these functions is constant at least on the blocks of π. But $B_w(\pi)$ may be computed from Proposition 5, therefore (4.1) is a simple consequence of the Möbius inversion theorem on partially ordered sets. Here $\mu_{\mathcal{P}}$ is defined inductively with $\mu_{\mathcal{P}}(\pi, \pi) = 1$, $\mu_{\mathcal{P}}(\pi, \sigma) = 0$ for $\pi > \sigma$, and

$$\mu_{\mathcal{P}}(\pi, \sigma) = -\sum_{\pi \leqslant \tau < \sigma} \mu_{\mathcal{P}}(\pi, \tau) \quad \text{for } \pi < \sigma. \quad \square$$

An exposition of the theory of Möbius inversion can be found in [1, 5].

Corollary 1. *Let $A_1(\pi)$ be the number of functions from X to Y with period π respect to group G, then*

$$A_1(\pi) = \sum_{\sigma \geqslant \pi} \mu_{\mathcal{P}}(\pi, \sigma)\, |Y|^{|\sigma|}. \tag{4.2}$$

Proof. If $g(C)$ is the enumerator of C, we denote with $g_1(C)$ the natural number obtained by putting $w(y) = 1$ for all $y \in Y$. Therefore, we will have $g_1(C) = |C|$. Now, if we operate this substitution in (4.1), then this will yield (4.2). $\square$

Corollary 2. *The number of aperiodic functions*

$$A_1(0) = \sum_{\sigma \in \Pi_n} \mu_{\mathcal{P}}(0, \sigma)\, |Y|^{|\sigma|} \tag{4.3}$$

is divisible by the order of G.

Proof. The formula (4.3) comes from (4.2) when $\pi = 0$. If furthermore f_1 and f_2

are aperiodic functions, we say that f_1 and f_2 are equivalent when there exists an $\alpha \in G$, such that $f_1\alpha = f_2$. So the set of aperiodic functions is partitioned in equivalence classes. Each of these classes contains exactly $|G|$ elements. In fact, because f_1 is aperiodic, we have $f_1\alpha \neq f_1\beta$ for every $\alpha \neq \beta$, belonging to G. It follows that $|G|$ divides $A_1(0)$. □

In the next example we give a combinatorial interpretation of the Jordan totient function.

Proposition 7. *Let $F_k(\pi)$ be the number of subsets T of G, with $|T| = k$, such that the period of $\langle T \rangle$ be π. Then*

$$F_k(\pi) = \sum_{\sigma \leq \pi} \mu_{\mathscr{P}}(\sigma, \pi) \binom{|\theta(\sigma)|}{k}. \tag{4.4}$$

Proof. In the same manner of the preceding cases, we set

$$G_k(\pi) = \sum_{\pi \leq \sigma} F_k(\sigma).$$

This number is easy to compute, in fact $G_k(\sigma) = \binom{|\theta(\sigma)|}{k}$, the binomial coefficient, and (4.4) follows by the Möbius inversion theorem. □

When we choose for G the cyclic group C_n, then it is possible to obtain the following

Corollary 3. *The number of k-subsets T of the cyclic group C_n that generate a cyclic permutation is*

$$c_{n,k} = \sum_{d|n} \binom{d}{k} \mu\left(\frac{n}{d}\right),$$

where μ is the classical Möbius arithmetical function.

In fact for this case we have $|\theta(\sigma)| = \binom{d}{k}$ when d is a divisor of n. Furthermore, it is $\mu(\sigma, \pi) = \mu(n/d)$. The number $c_{n,k}$ may be expressed function of the Stirling numbers of first kind $s(n, h)$ and of the Jordan totient function $J_h(n) = \sum_{d|n} d^h \mu(n/d)$. In conclusion we can write the identity

$$k!\, c_{n,k} = \sum_{h=0}^{k} s(k, h) J_h(n).$$

References

[1] M. Aigner, Combinatorial Theory (Springer, Berlin, 1979).
[2] G. Birkhoff, Lattice Theory, Vol. 25, 3rd edition (Providence: Amer. Math. Soc. Coll. Publ. 1967).

[3] M. Cerasoli, Calcolo combinatorio, Japadre Ed. L'Aquila (1983).
[4] M. Cerasoli, Poisson randomization in occupancy problems, J. Math. Anal. Appl. 94 (1983) 150–165.
[5] G.-C. Rota, On the foundations of combinatorial theory: I. Theory of Möbius functions, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete, 2 (1964) 340–368.
[6] G.-C. Rota, Baxter algebras and combinatorial identities, II, Bull. Amer. Math. Soc. 75 (1969) 330–334.
[7] G.-C. Rota and B. Sagan, Congruences derived from group action, Europ. J. Combina. 1 (1980) 67–76.
[8] G.-C. Rota and D. A. Smith, Enumeration under group action, Annali Scuola Normale Superiore–Pisa Classe di Scienze 4 (1977) 637–646.